

1 CLAIMS

2 What is claimed is:

3 1. A method for detecting an attack on a data processing
4 system, the method comprising, in the data processing
5 system:

6 providing an initial secret;

7 binding the initial secret to data indicative of an initial
8 state of the system via a cryptographic function;

9 recording state changing administrative actions performed on
10 the system in a log;

11 prior to performing each state changing administrative
12 action, generating a new secret by performing the
13 cryptographic function on a combination of data indicative
14 of the administrative action and the previous secret, and
15 erasing the previous secret;

16 evolving the initial secret based on the log to produce an
17 evolved secret;

18 comparing the evolved secret with the new secret;

19 determining that the system is uncorrupted if the comparison
20 indicates a match between the evolved secret and the new
21 secret; and

22 determining that the system is corrupted if the comparison
23 indicates a mismatch between the evolved secret and the new
24 secret.

1 2. A method as claimed in claim 1, wherein the
2 cryptographic function comprises a one-way hash function.

3 3. A method as claimed in claim 2, wherein the hash
4 function comprises an exponentiation function.

5 4. A method as claimed in claim 1, wherein the
6 cryptographic function comprises a public/private key pair.

7 5. A method as claimed in claim 1, comprising receiving
8 the initial secret from a system administrator.

9 6. A data processing system comprising:

10 a processor;

11 a memory connected to the processor; and

12 detection logic connected to the processor and the memory,
13 the detection logic, in use:

14 providing an initial secret;

15 binding the initial secret to data indicative of an
16 initial state of the system via a cryptographic
17 function;

18 recording state changing administrative actions
19 performed on the system in a log;

20 prior to performing each state changing administrative
21 action, generating a new secret by performing the
22 cryptographic function on a combination of data
23 indicative of the administrative action and the
24 previous secret, and erasing the previous secret;

1 evolving the initial secret based on the log to produce
2 an evolved secret;

3 comparing the evolved secret with the new secret;

4 determining that the system is uncorrupted if the
5 comparison indicates a match between the evolved secret
6 and the new secret; and

7 determining that the system is corrupted if the
8 comparison indicates a mismatch between the evolved
9 secret and the new secret.

10 7. A system as claimed in claim 6, wherein the
11 cryptographic function comprises a one-way hash function.

12 8. A system as claimed in claim 7, wherein the hash
13 function comprises an exponentiation function.

14 9. A system as claimed in claim 6, wherein the
15 cryptographic function comprises a public/private key pair.

16 10. A system as claimed in claim 6, wherein the detector
17 logic receives the initial secret from a system
18 administrator.

19 11. A computer program element comprising computer program
20 code means which, when loaded in a processor of a computer
21 system, configures the processor to perform a method as
22 claimed in claim 1.

23 12. An article of manufacture comprising a computer usable
24 medium having computer readable program code means embodied
25 therein for causing detection of an attack on a data
26 processing system, the computer readable program code means
27 in said article of manufacture comprising computer readable

1 program code means for causing a computer to effect the
2 steps of claim 1.

3 13. A program storage device readable by machine, tangibly
4 embodying a program of instructions executable by the
5 machine to perform method steps for detecting an attack on a
6 data processing system, said method steps comprising the
7 steps of claim 1.

8 14. A computer program product comprising a computer usable
9 medium having computer readable program code means embodied
10 therein for causing a data processing system, the computer
11 readable program code means in said computer program product
12 comprising computer readable program code means for causing
13 a computer to effect the functions of claim 6.

14 15. A method for cryptographic entangling of state and
15 administration in a data processing system, the method
16 comprising:

17 initializing the system by generating an initial secret

18 releasing binding data;

19 binding the binding data to the initial secret;

20 updating the initial secret in advance of an administrative
21 action by computing a new secret;

22 erasing the initial secret together with any information
23 from which the initial secret might be derived;

24 recording data indicative of the administrative action;

25 permitting execution of the administrative action;

1 offering a proof that the new secret corresponds to the
2 initial secret as it has evolved according to a record of
3 administrative actions.

4 16. A method as recited in claim 15, wherein the step of
5 offering retrieves the initial secret via a request for
6 entry of the initial secret by a system administrator,
7 retrieving the record of administrative actions previous
8 stored; and

9 evolving a candidate secret for the initial secret based on
10 the record of administrative actions retrieved;

11 comparing the candidate secret with a current secret;

12 if the candidate secret matches the current secret,
13 reporting that the data processing system is still in an
14 uncorrupted state, and

15 if the candidate secret does not match the current secret,
16 reporting that the data processing system is in a
17 potentially compromised state.

18 17. A method as recited in claim 15, further comprising
19 permitting detection of any Trojan horse within the system.

20 18. A method as recited in claim 15, wherein the initial
21 secret is supplied via a secure communication channel.

22 19. A method as recited in claim 15, wherein the binding
23 data takes different forms depending on the data processing
24 system, an application of the data processing system, and a
25 trust mechanisms associated with communication of the
26 initial secret.

1 20. A method as recited in claim 15, wherein the
2 administrative action is an action taken from a group of
3 actions consisting of: updating of system executable code;
4 updating of system libraries; installation of kernel
5 modules; reading of files such as those used to store system
6 states during rebooting operations; alteration of
7 configuration files; alteration of system run-level codes;
8 writing to or reading from peripheral devices; and any
9 combination of these actions.

10 20. A method as recited in claim 15, wherein the step of
11 computing the new secret includes applying a one way
12 function to a combination of a previous secret and data
13 indicative of the administrative action.

14 21. An article of manufacture comprising a computer usable
15 medium having computer readable program code means embodied
16 therein for causing cryptographic entanglement of state and
17 administration in a data processing system, the computer
18 readable program code means in said article of manufacture
19 comprising computer readable program code means for causing
20 a computer to effect the steps of claim 15.

21 22. A program storage device readable by machine, tangibly
22 embodying a program of instructions executable by the
23 machine to perform method steps for cryptographic entangling
24 of state and administration in a data processing system,
25 said method steps comprising the steps of claim 15.